11/7/2023

VectorZero Incubatenergy Labs Whitepaper

Evaluating Active Data Vault's Cybersecurity & Useability for Utilities

Cris Martin
VECTORZERO

Contents

Executive Summary

Introduction: Electric Power Research Institute (EPRI), the world's preeminent independent, non-profit energy research and development organization, engaged with VectorZero for this pilot and subsequent whitepaper. VectorZero is a Reston, VA-based cybersecurity and data governance startup under the technical leadership of former US intelligence community officers. The collaboration came about via EPRI's Incubatenergy Labs (IEL) program, of which VectorZero is a member of the 2023 cohort.

This whitepaper provides an objective overview of the outcomes and insights resulting from the EPRI Knoxville Cyber Lab team's extensive assessment of VectorZero's Active Data Vault (ADV). The evaluation primarily centers on ADV's capabilities in augmenting security and usability, along with its compatibility with prevalent utility applications, software platforms, and datasets in the electric power sector.

Objective: The primary objective of this collaborative pilot project was to gauge ADV's potential to reinforce cybersecurity and data governance within the electric power industry. EPRI aimed to establish its adaptability, resilience, and value as an element in the cybersecurity framework of utility infrastructure.

Key Findings:

1. **Enhanced Cybersecurity:** ADV exhibited commendable prowess in enhancing cybersecurity measures when tested in the Knoxville Lab. It excelled in encrypting data, storing files, and securely running common utility applications. Our tests concluded ADV could contribute to risk reduction associated with cyber threats and data breaches.

2. **Usability:** During the pilot, ADV proved to be user-friendly and seamlessly integrated with EPRI's requested utility applications and datasets. Its intuitive interface and compatibility with commonly used software indicate it could be a useful tool for professionals and knowledge works across various departments within a utility.

3. **Data Governance:** ADV's data governance features streamlined data management in our lab use case, which was testing ADV's logging feature in conjunction with Splunk. ADV facilitated complete logs of all user and software actions for intuitive data tracking, audit trails, and access controls, thereby demonstrating capabilities which indicated probable adherence to industry regulations and common enterprise protocols.

Conclusion: VectorZero's Active Data Vault (ADV) has emerged as a compelling solution for addressing cybersecurity and data governance requirements within the electric power industry. EPRI's pilot program demonstrated ADV's capacity to enhance security, usability, and data management while seamlessly integrating with essential utility applications and datasets. The successful outcome of this collaborative effort underscores ADV's potential in fortifying critical infrastructure and ensuring data integrity within the electric power sector.

The insights gathered from this evaluation serve as a foundation for potential future collaborations between VectorZero and utility companies, outlining a path to establish new benchmarks in cybersecurity and data governance practices within the industry. As the electric power sector continues to evolve, ADV is poised to contribute to bolstering digital defenses and safeguarding sensitive data assets.

Utility Cybersecurity Challenges

There are a number of cybersecurity challenges facing utilities, which we will briefly summarize here.

General Cybersecurity Challenges

A Skybox Security research study found that 87% of utilities have experienced at least one security breach in the past 36 months.

Customer Data Leakage

Customer data accounted for 58% of all data stolen from energy and utility firms in 2021, according to a 2022 data breach investigations report from Verizon.

NERC CIP Compliance

If utilities are not in compliance with North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), they can be fined up to $1,000,000 per day. The largest NERC CIP fine ever levied was $10,000,000 in 2019. Pressure to remain in strict compliance can present challenges for utilities that want to pursue innovative experimentation.

NERC CIP Compliant Cloud Infrastructure & Migration

Another challenge to NERC CIP compliance exists for utilities who would like to migrate to the commercial cloud. While there may be economic, operational, and even security benefits to cloud migrations, there are technical and economic obstacles to doing so. For example, bringing on an entire team of developers and security professionals to erect a compliant, secure, cloud infrastructure.

Zero Trust Implementation & Compliance

In addition to the March ’23 federal cybersecurity strategy, the administration issued an executive order in May ’21 which mandated that all critical infrastructure go Zero Trust by 2023. Despite the mandate, according to IBM Security’s 2022 Cost of a Data Breach Report, only 1 in 5 critical infrastructure organizations have adopted Zero Trust.

Data Governance & Sharing Data With 3rd Party Vendors

Trusting 3rd parties presents risk for any enterprise organization. Yet vendors, whether they are an innovative startup or a decades-long partner, they need data. At the same time, it is very difficult for utilities to tolerate the added risk of sharing real data. This forces utility R&D teams to often use “sand box” data, for pilots, which makes them less informative and impactful – especially around scaling decisions.

Integration of Security Software & Applications Throughout the Enterprise

Heterogeneous applications, data types, devices and security tools coming from different vendors, sources, and formats do not always integrate smoothly. This presents a challenge for professionals across the enterprise when attempting to integrate their various tools into one single user interface.

Compromised Edge Devices

Smart grid, remote work-from-home networks, and generally having a wide spanning enterprise with thousands of users and devices present numerous attack surfaces. A single compromised device at the edge can spell disaster for a utility if exploited properly.

Advanced Persistent Threats (APTs)

In 2022 Utilities were plagued by APTs. These are long running hacks where utilities breach a network and then conduct recon, pry for further access, and wait to strike until data is at its most vulnerable. According to IBM Security’s 2022 Cost of a Data Breach Report, it took utilities an average of 204 days to detect a breach. Then, it took another 69 average days to remediate those breaches, meaning that the average shelf life of a breach was 273 total days.

Ransomware

According to Verizon’s 2022 Data Breach Investigations report, 179 utilities had a confirmed data disclosure incident in 2022. To scope the entire industries ransomware for 2022, we can multiple the 179 breaches times IBM’s 2022 estimated average cost per breach, which was $4.82 million:

179 breaches x $4.82mm = Estimated $863m lost in 2022

Espionage

IBM reported 22% of 2022 cyber attacks on critical infrastructure were espionage related. This indicates the adversaries are tenacious, sophisticated, and well-resourced.

About VectorZero Active Data Vault

VectorZero Active Data Vault (ADV) is a SaaS, zero trust, high-assurance infrastructure that is stood up in hours and in just three clicks. With thousands of security controls as per NIST 800-53-5 or NERC CIP, VectorZero enclaves are designed with the relevant security frameworks in mind. ADV then exceeds these standards to address residual risk via six (6) key features:

1. Automated Moving Target Defense – VectorZero ephemeral networks are not only designed to be stood up in hours, they can also be deprovisioned in a single click. This action saves the compartment in secure storage, or in a concurrent infrastructure, where the compartment can then be reopened moments later in a brand new (and thus totally clean) network.

   These infrastructure moves counter advanced persistent threats since each move orchestrates changes to IP addresses, ports, and additional componentry. No adversary can establish a foothold in a network that is constantly "frequency hopping". This capability is enhanced by machine learning and pattern recognition software, which are regularly scanning to detect threat actors and will trigger alerts to coordinate infrastructure moves as appropriate.

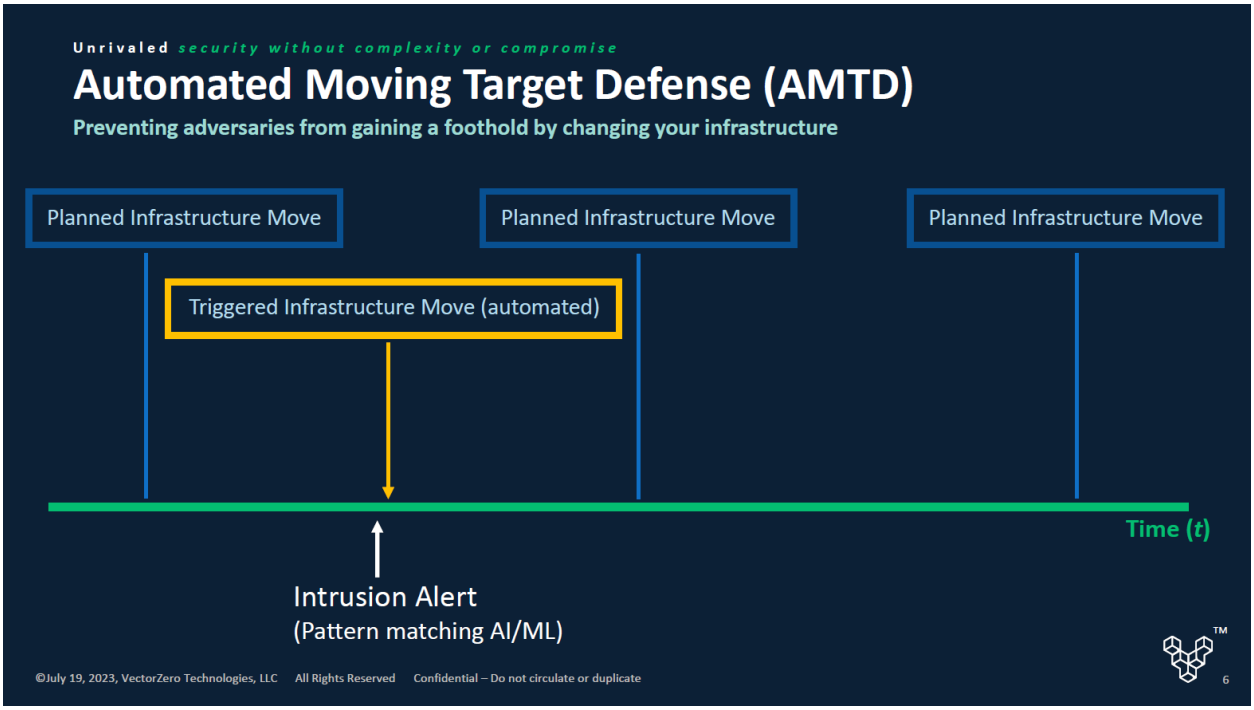

Figure 1 – Automated Moving Target Defense for countering Advanced Persistent Threats

An added benefit of ephemeral infrastructure is its simple implementation of zero trust. ADV Infrastructure can be tested incrementally one team at a time. Scaling to additional teams requires just a few clicks to set up an ADV environment which can then be intuitively operated by non-technical users. Once an ADV is deployed, the

organization would be well on its way to a zero trust environment.

2. Confidential Computing – Incumbent technologies only encrypt data at rest and in transit; ADV is unique in that it also encrypts data in use when running analytics, AI, or ML. This capability counters memory unsafety, side channel attacks, kernel vulnerabilities, and more.

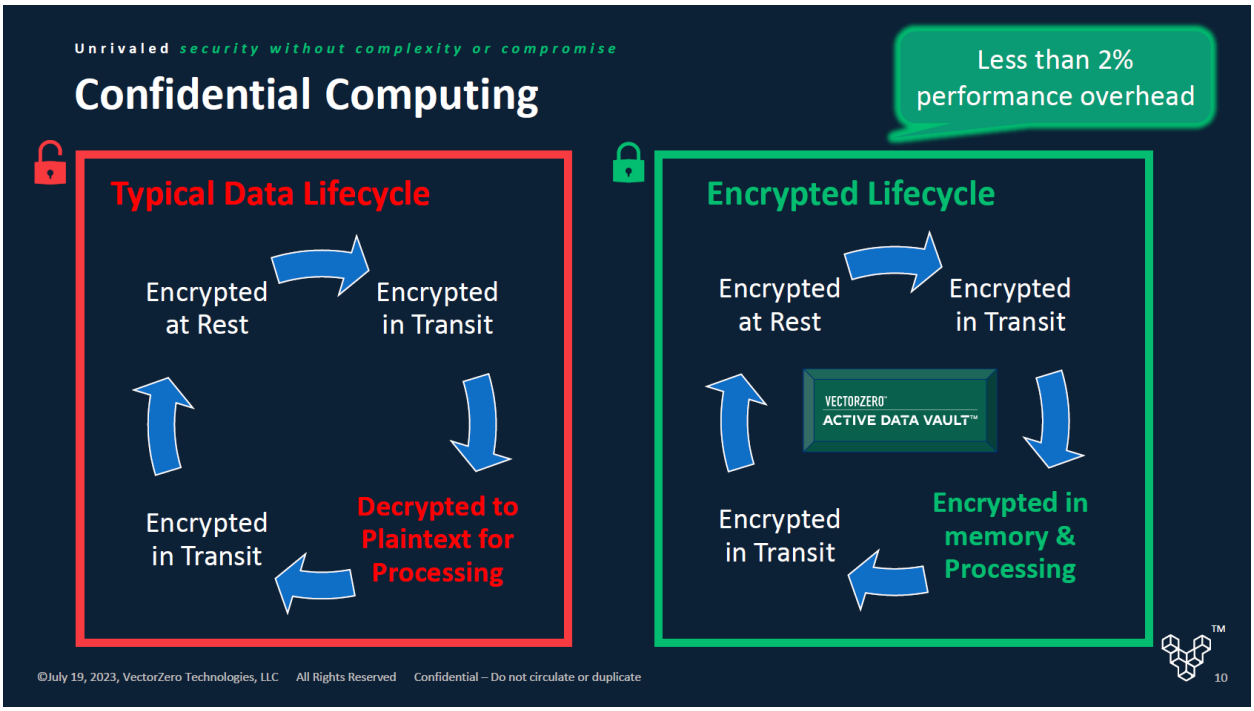

Figure 2 – Confidential computing encrypts data in memory & processing

It further counters insider threat since data is accessible to authorized workloads, yet unreadable to platform administrators, hypervisors, data scientists, data engineers, and even cloud service provider employees who have physical access to the machines.

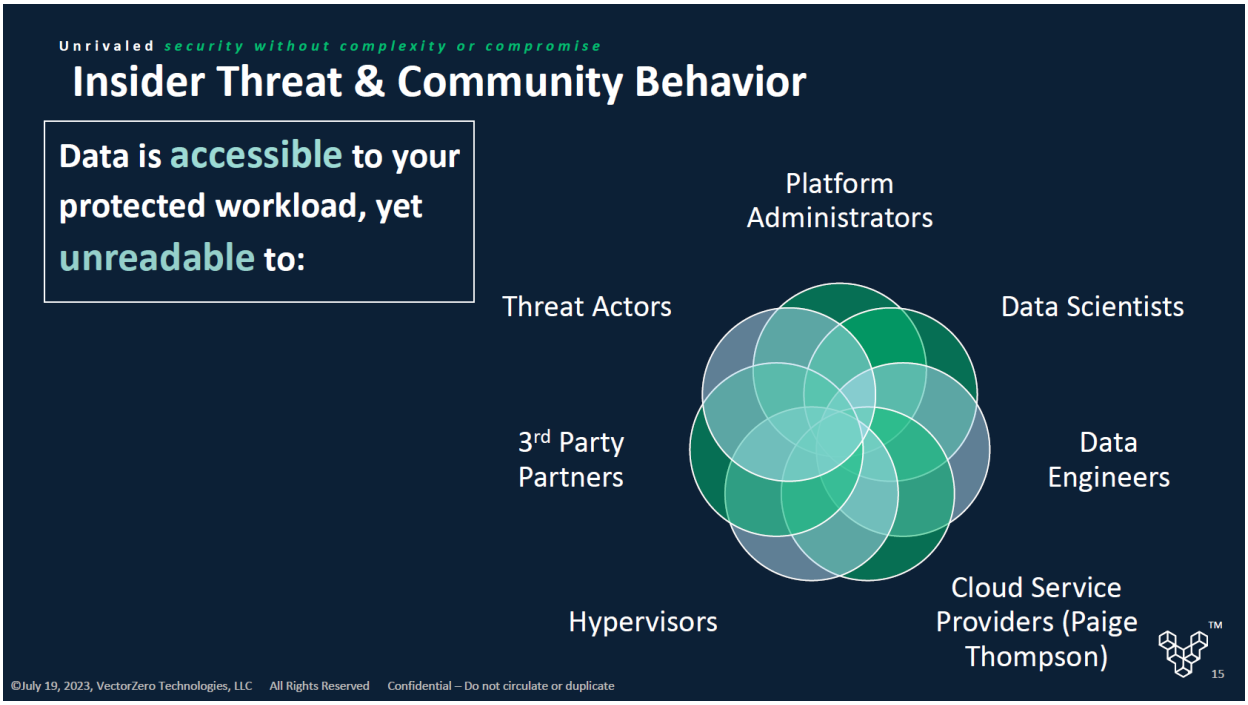

Figure 3 – Confidential computing counters insider threat

3. Secure Multiparty Computation (SMPC) - Beyond security, confidential computing enables SMPC. SMPC is a novel capability that is applicable in many multiparty scenarios. Generally, it enables parties to jointly run analytics on their aggregate data without revealing their individual private inputs to each other. Said another way, SMPC is a promising technology to enable utilities to keep their data private while utilizing 3rd party vendor code.

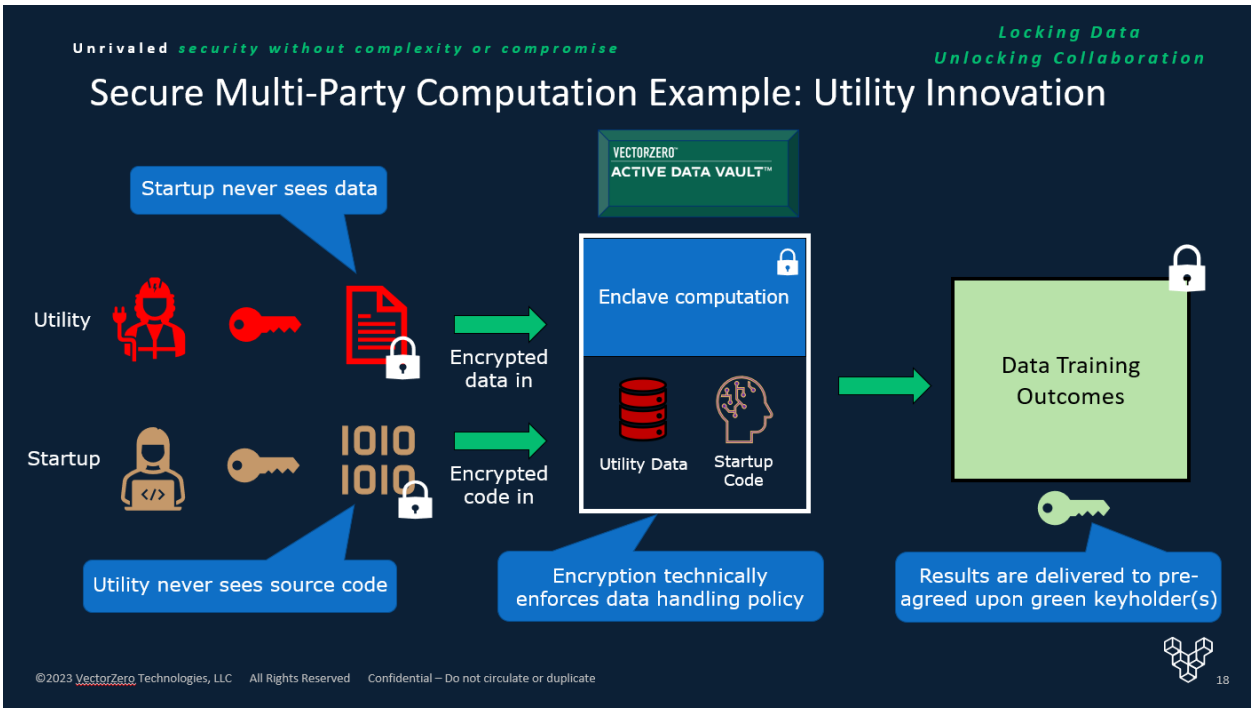

Figure 4 – SMPC streamlines data governance, keeping utility data private from 3rd party vendors

4. Quantum Hardened – ADV is engineered to meet post-quantum standards as set forth by FIPS 140-2 Level 3 and thus counters HNDL threats. Further, it is designed to be easily upgraded in hours if emergent encryption methods are developed or required by customers.

5. Supply Chain Security & Governance – ADV does not release sensitive data unless the supply chain is verified as trustworthy via attestation signatures. This mathematical method uses cryptographic measurements to verify more, trust less, when it comes to 3rd party vendors. This attestation authentication is foundational to security and enables organizations to compare server claims against a machine-readable version of their corporate security policy. This includes automated compute, data, or key release based on adjudication of attestation evidence.

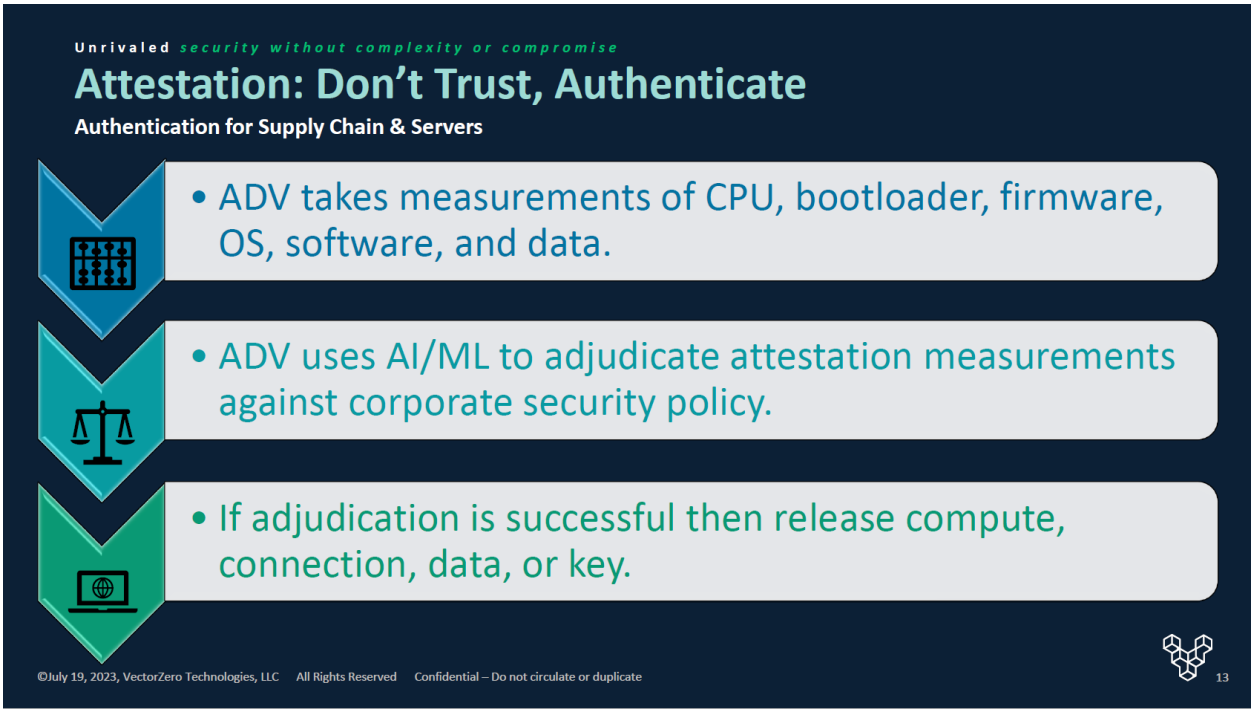

Figure 5 – Attestation automatically adjudicates server requests against corporate security policies

6. Frontroom Virtual Machines – Known as 'frontrooms', ADV's virtual desktop is an intuitive user interface that provides access to a full computer desktop experience. While ADV users may not notice a difference between a frontroom and a regular desktop, the differentiation is that no files are ever resident on their device. Rather, users are interacting with a video stream of the file. This means that if a malicious actor penetrates the user's device, at most only pixels on the screen can be compromised, but not entire files.

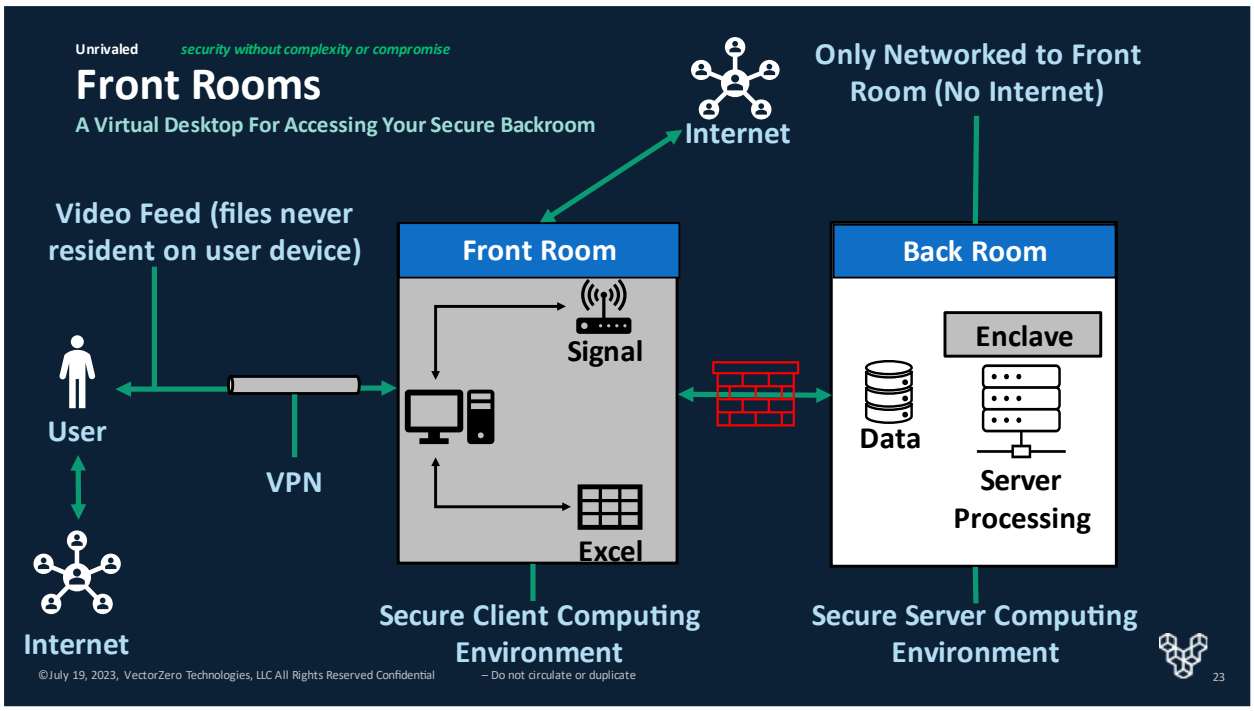

Figure 6 – ADV frontrooms ensure that no sensitive files are resident on user devices

About The Pilot

Background

Through Incubatenergy Labs, EPRI and a group of leading utilities engaged early stage startup companies to demonstrate and deploy innovative solutions in targeted areas. Applicants needed to be past the early development stage, but not commercially deployed. VectorZero was selected by EPRI to demonstrate its cloud-native Active Data Vault™ (ADV) technology for cybersecurity & data governance applications. The demonstration was to be carried out at the EPRI Knoxville Cyber Lab.

About the EPRI Knoxville Cyber Lab

The CSRL (Cyber Security and Research Laboratory) boasts an impressive array of resources, with over $2.5 million worth of cutting-edge hardware, software, and other equipment at its disposal. This extensive collection comprises 172 devices sourced from over 30 renowned manufacturers. These assets are meticulously configured to support multiple SCADA (Supervisory Control and Data Acquisition) protocols, including DNP3, IEC 61850, Sunspec MODBUS, IEEE C37.118, IEC 104, and IEC 101, ensuring comprehensive compatibility and robust functionality.

In 2023, the CSRL successfully delivered 15 crucial lab-related projects, contributing to its reputation as a leading facility for advanced research and development. The CSRL encompasses specialized lab areas, including the Smart Grid Substation Lab, Integrated Security Operations Center (ISOC), and the DER and Grid Edge Cyber Security Area, each dedicated to fostering innovation and resilience in critical infrastructure systems.

One of the lab's notable achievements is the daily logging of over 200,000 SCADA events, enabling the thorough evaluation of new technologies and architectures. In addition, the CSRL is renowned for its expertise in penetration testing and forensic analysis of embedded systems, further enhancing its role in fortifying cybersecurity and resilience within the energy sector.

Scope of Work & Project Limitations

This pilot project was conducted at the EPRI Knoxville Cyber Lab over a period of sixteen (16) weeks from July ’23 to Nov ’23. During that time, EPRI cybersecurity Subject Matter Experts (SMEs) extensively tested ADV to validate ADV’s applicability to utility operations. While member utilities and VectorZero informed the tests, all decisions pertaining to tests conducted were at the sole discretion of EPRI. EPRI SMEs selected the applications to install, workloads to test, and data to utilize.

One notable limitation that was placed on EPRI pertained to penetration testing. Since ADV is a cloud-native product in the Amazon Web Services (AWS) cloud, any penetration testing was limited to be in compliance with AWS terms of service.

Another notable limitation was testing the integration of ADV with other 3rd party vendors such as Splunk, Schweitzer Engineering Laboratories (SEL), GE, and others. While VectorZero demonstrated its ability to integrate ADV with software products designed by these 3rd party vendors, those vendors did not directly participate in the pilot, no licenses of their software were purchased or dedicated to this pilot.

Identified Utility Use Cases, Tests Conducted, & Results

Based on the judgement of EPRI Knoxville cybersecurity SMEs, and in consultation with VectorZero, the following use cases were identified and tested during this pilot. As a result of the that Larry Burnette, EPRI Cyber Security Engineer, produced this video and voiceover demonstrating his use of ADV. This video covers many of the use cases mentioned below.

Highly Secure Configuration File Backups

Utilities have very large configuration files that are constantly being updated. These files are a crucial component of a utility's operations where the configurations manage and control various aspects of their systems and infrastructure. They contain settings, parameters, and instructions which dictate how different components of a utility's systems should behave, making them a ripe target for ransomware. For example, when the group known as DarkSide attacked Colonial Pipeline, they compromised Colonial Pipeline's configuration files.

At the Knoxville Cyberlab, EPRI used VectorZero Active Data Vault as an isolated and secure backup location for configuration files. We installed SEL Quickset and SEL RTAC into VectorZero frontrooms for secure access to these software products. We then used the SEL products in the frontroom, where they ran at typical speeds and useability. Lastly, we were able to upload and download configuration files as needed throughout the test.

In summary, the result of this test was an intuitive and highly secure means to access, edit, upload, download, and backup configuration files. The implications of backing up configuration files in an ADV are that utilities will have up to date configuration files isolated from their production network. In the event that a malicious actor compromises a utility's perimeter and production configuration files, the utility should be able to revert to recent configuration files saved elsewhere in the ADV.

NERC CIP Compliant Cloud + Cloud Migration

Having a NERC CIP compliant cloud environment could be immensely beneficial to a utility. The enterprise could benefit across many metrics such as cost savings, scalability, flexibility, agility, disaster recovery and business continuity, security, and resource efficiency. At the same time, to develop a NERC CIP compliant cloud in house could be an expensive, time consuming, and risk laden endeavor for a utility.

Out of the box, VectorZero ADV scored in the 90% range on the AWS NERC CIP Conformance Pack. With this impressive score throughout the pilot, we believe Active Data Vault could be a viable path forward to establish NERC CIP compliant cloud environments for utilities.

Furthermore, VectorZero our team at the EPRI Knoxville Cyber Lab found ADVs to be intuitive and user-friendly environments for knowledge workers. The no-code, point and click design did not impose any learning curve for our staff, making for simple implementation with minimal training across a workforce.

Zero Trust Compliance & Implementation

VectorZero ADV aligns with the NIST 800-207 standard for zero trust. This Zero Trust security framework requires all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

Furthermore, Zero Trust seeks to limit the "blast radius," minimizing impact if an external or insider breach does occur. We believe VectorZero is ideal for Zero Trust implementation because each ADV enclave is isolated from the others. Thus, utilities can onboard incrementally, one team and one ADV at a time. As each new team joins, they won't have access to other teams' ADVs. This architecture should contain any breach and serve as a means to prevent malicious actors from lateral movement between ADVs.

One test we ran during this pilot was to view ADV's logs in Splunk. It was not difficult or time consuming for our staff to download ADV's logs, then upload and view them in Splunk. Based on this experience, a cybersecurity professional could continue to use Splunk as a single pane of glass Security Information and Event Management (SIEM) tool.

Data Governance & Data Sharing

The process to have a utility share data can often involve hours spent filling out forms and communicating with stakeholders across the enterprise: cyber, digital, supply chain, regulatory, legal, etc. While these processes reduce risk, they also have the potential to slow down innovation, R&D, and other high impact work. What if all stakeholders involved could achieve their goals simultaneously?

VectorZero claims that their SMPC feature can provide a technical means of doing so. By keeping data encrypted at all times with confidential computing, data can remain accessible to authorized workloads while remaining unreadable to users. This should provide a means of verifiable privacy while still enabling joint computations.

EPRI was unable to test this SMPC feature during the course of this trial due to license issues. Our issue was that VectorZero simply enables the computation, but it is 3rd party software such as an AI, ML, or analytics tool that would ultimately run the computation. Since we didn't have such a tool available, we were unable to test this feature. An ideal future pilots or test would scope within its requirements what tools, policies, and relationships in order to validate this feature and use case.

However, we were able to run Packet Capture (CPAP) test with VectorZero ADV to see if the data is encrypted when uploading or downloading from the environment. We used Wireshark to conduct this specific test and were able to confirm the encryption work as intended for data in transit.

Virtual Machines for Secure Edge

As work from home becomes more common, it increases the attack surfaces IT professionals have to consider. Users can have countless devices on their home wifi network, each of which presents a vector of attack to compromise that user's device or communications.

VectorZero frontrooms could be a viable counter to these threats. A frontroom is a virtual machine, which is a software-based emulation of a physical computer. The distinction between a frontroom and a typical virtual machine is the VectorZero frontroom can connect directly to the VectorZero ADV, giving the user access to edit and use files that are stored in a highly secure environment. At the same time, these files are never resident on the user's device. Rather, the user is interacting with a video stream of their file.

Thus, from the user perspective, it looks and feels like they are interacting with their file as normal. However, from a malicious actor's perspective, if the user device is compromised, at most, the bad actor would see whatever data is visible on the screen. Notably, the bad actor would not be able to steal or compromise the entire file itself though.

During the course of the pilot, we test VectorZero frontrooms extensively and found them to interact seamlessly in all regards. We had no issues connecting to the VectorZero server environment, nor did we have any complicated user experience while interacting with the frontroom feature.

Conclusion

In this comprehensive whitepaper, we have explored the results and insights derived from a collaborative pilot project between the Electric Power Research Institute (EPRI) and VectorZero, a cybersecurity and data governance startup. The primary objective of this project was to evaluate VectorZero's Active Data Vault (ADV) and its potential to enhance cybersecurity and data governance within the electric power industry.

The results of this pilot project demonstrate that VectorZero's Active Data Vault is a compelling solution for addressing cybersecurity and data governance challenges within the electric power industry. Its adaptability, security features, and user-friendly interface make it a viable asset for consideration by utility companies seeking to enhance their digital defenses and safeguard sensitive data assets.

The insights gained from this collaboration pave the way for potential future collaborations between VectorZero and utility companies, setting the stage for advancing cybersecurity and data governance practices within the industry. As the electric power sector continues to evolve, ADV is poised to play a crucial role in securing critical infrastructure and maintaining data integrity. It is an innovative step towards ensuring the resilience and security of the electric power grid in an increasingly interconnected and digitized world.